Chapitre 4 – Groupes

Dans ce chapitre, nous allons aller un peu plus loin avec les groupes, en préparation du chapitre suivant et aussi parce que certains des résultats ci-dessous sont des classiques.

Il faut avoir en tête quelques exemples de groupes, pour apprécier les théorèmes. Nous allons surtout privilégier les groupes finis ici. Il y a donc les groupes abéliens finis, qui – on le sait depuis le chapitre précédent – sont des produits de groupes cycliques. Il y a aussi le groupe diédral D_8, que nous allons examiner dans les exercices : il est engendré par deux éléments r et s, avec $s^2 = r^4 = 1$ et $srs = r^{-1}$, et il compte en tout huit éléments, qui sont $1, r, r^2, r^3$ (ce sont les rotations, dans l'interprétation géométrique que l'on a de D_8) et s, sr, sr^2, sr^3 (qui sont des symétries par rapport à des droites).

Ensuite, nous avons le groupe Q_8. Celui-ci est un sous-groupe de $\mathbb{H}^\times$, où $\mathbb{H}$ est le corps des quaternions, vu dans les exercices ; on définit $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, il comporte donc 8 éléments, avec $i^2 = j^2 = k^2 = ijk = -1$.

Enfin, dernier exemple important, celui de S_n, le groupe symétrique de degré n, dont les éléments sont les permutations de l'ensemble $\{1, 2, \ldots, n\}$.

§1 Les classes à gauche

Lorsque H est un sous-groupe de G, nous allons définir un ensemble G/H qui va être utile à plusieurs titres. Dans certains cas, G/H sera lui-même un groupe, mais nous n'utiliserons pas énormément ces quotients, finalement. Par contre, on aura besoin de G/H quand nous parlerons des actions de groupes, et également dans un argument classique de comptage qui vient tout de suite.

Premières définitions

Définition 1. Soit G un groupe, et $H \subset G$ un sous-groupe. Pour $g \in G$, on note

$$gH := \{gh \mid h \in H\},$$

et on pose

$$G/H := \{gH \mid g \in G\}.$$

Lorsque G et H sont fixés une fois pour toutes, on note $\overline{g}$ pour gH. Avec cette notation, on a

$$G/H = \{\overline{g} \mid g \in G\}.$$

Jusqu'ici, c'est simplement la notation pour les modules quotients qui a changé ($v + U$ devient gH). Est-ce qu'on peut toujours espérer qu'il y ait une structure de groupe sur G/H, de sorte que l'application $p\colon G \longrightarrow G/H$ définie par $g \mapsto \overline{g}$ soit un homomorphisme ? La réponse est non, pas toujours.

Définition 2. Soit H un sous-groupe de G. On dit que H est *distingué* dans G lorsque, pour tout $g \in G$, on a $gHg^{-1} \subset H$.

Remarque. Dans ce cas, en prenant g^{-1} on a $g^{-1}Hg \subset H$ d'où $H \subset gHg^{-1}$ (en multipliant à gauche par g et à droite par g^{-1}), donc en fait on a une égalité $gHg^{-1} = H$ pour tout $g \in G$.

Exemple 3. Si G est abélien, il est clair que tous ses sous-groupes sont distingués. Si $G = S_n$ (le groupe symétrique sur n symboles), et si $H = \{Id, (1,2)\}$, alors $gHg^{-1} = \{Id, (g(1), g(2))\}$ (nous ferons des révisions sur les permutations plus tard ; c'est juste pour avoir un exemple). Clairement, ce H n'est pas distingué en général (prendre $n \geq 3$ et une permutation g telle que $g(1) = 3$).

Plus important :

Lemme 4. *S'il existe un homomorphisme $\varphi\colon G \longrightarrow G'$ tel que $H = \ker \varphi$, alors H est distingué.*

Démonstration. En effet pour $h \in H$ et $g \in G$

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1\,,$$

d'où $ghg^{-1} \in H$. □

Conclusion : si H n'est pas distingué, il n'est pas possible que H soit le noyau de quoi que ce soit, donc une structure de groupe sur G/H comme espéré ci-dessus ne peut pas exister.

Mais c'est le seul obstacle :

Lemme 5. *Supposons que H soit un sous-groupe distingué de G. Alors il existe une structure de groupe sur G/H, et une seule, telle que l'application naturelle $G \longrightarrow G/H$ soit un homomorphisme. Son noyau est H.*

Démonstration. Si X et Y sont des parties de G, on définit

$$XY = \{xy \mid x \in X, y \in Y\}\,.$$

Or on peut vérifier que, pour $\sigma, \tau \in G$, on a

$$(\sigma H)(\tau H) = \sigma\tau H\,. \qquad (*)$$

En effet, l'inclusion $\sigma\tau H \subset (\sigma H)(\tau H)$ est évidente (car $1 \in H$), et pour la réciproque, on écrit

$$\sigma h_1 \tau h_2 = \sigma\tau(\tau^{-1}h_1\tau)h_2 \in \sigma\tau H$$

puisque $\tau^{-1}h_1\tau \in H$. D'où $(\sigma H)(\tau H) \subset \sigma\tau H$.

Ceci nous donne une multiplication sur G/H, et (*) montre que $\overline{\sigma}\,\overline{\tau} = \overline{\sigma\tau}$. On en déduit facilement, comme dans le cas des modules, que l'on a bien une structure de groupe sur G/H. La démonstration que le noyau de p est H est également similaire à celle dans le cas des modules. □

Très souvent, nous utiliserons la lettre N pour un sous-groupe distingué de G (c'est parce qu'on dit parfois « groupe normal » au lieu de « groupe distingué »).

Proposition 6. *Soit N un sous-groupe distingué de G, et soit $\varphi\colon G \longrightarrow H$ un homomorphisme tel que $N \subset \ker\varphi$. Alors il existe un unique homomorphisme $\overline{\varphi}\colon G/N \longrightarrow H$ tel que $\overline{\varphi}(\overline{g}) = \varphi(g)$ pour tout $g \in G$. De plus, si φ est surjective et si $N = \ker(\varphi)$, alors $\overline{\varphi}$ est un isomorphisme, ce qu'on résume en*

$$G/\ker(\varphi) \cong \mathrm{Im}(\varphi)\,.$$

Démonstration. Comme pour les modules. □

Exemple 7. Vous connaissez sans doute l'homomorphisme dit « de signature »

$$\varepsilon\colon S_n \longrightarrow \{\pm 1\}\,,$$

et vous devez savoir que son noyau est appele le *groupe alterné* de degré n, noté A_n. On a donc

$$S_n/A_n \cong \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}\,.$$

Le théorème de Lagrange

Comme promis, considérer les classes à gauche, c'est-à-dire les éléments de G/H, peut servir à d'autres choses qu'à former des quotients. Commençons par :

Lemme 8. *Soit xH et yH deux éléments de G/H. Si $xH \cap yH \neq \emptyset$, alors $xH = yH$.*

Démonstration. Supposons que $z \in xH \cap yH$. Alors $z = xh$ pour un $h_1 \in H$, et $z = yh_2$ pour un $h_2 \in H$, par définition. Donc $x = zh_1^{-1} = yh_2h_1^{-1} \in yH$; donc $xH \subset yH$, clairement ; et de manière symétrique, on a aussi $yH \subset xH$, d'où $xH = yH$. □

En corollaire, nous avons

Théorème 9 (Lagrange)**.** *Soit G un groupe fini, et soit H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G. Plus précisément, nous avons*

$$\frac{|G|}{|H|} = |G/H|\,.$$

Démonstration. Si $g \in G$, on a bien sûr $g \in gH$, donc G est l'union de tous les ensembles gH, où g parcourt G. Mais d'après le lemme, cette union est *disjointe*. Si $k = |G/H|$, le groupe G est donc l'union disjointe de $x_1H, x_2H, \ldots, x_kH$, pour des $x_i \in G$ (non-uniques !), de sorte que

$$|G| = |x_1H| + \cdots + |x_kH|\,. \qquad (*)$$

Mais chaque ensemble gH est en bijection avec H : considérer l'application $H \longrightarrow gH$ définie par $h \mapsto gh$, d'inverse $x \mapsto g^{-1}x$. Donc $|gH| = |H|$ pour tout g, et en particulier $|x_iH| = |H|$ pour tout i. De l'égalité (*) on tire alors $|G| = k|H|$. □

Corollaire 10. *Si $g \in G$, alors l'ordre de g divise l'ordre de G. En particulier, on a $g^{|G|} = 1$.*

Démonstration. Le théorème de Lagrange appliqué à $H = \langle g \rangle$ donne la première phrase. Si k est l'ordre de g, on a donc $|G| = kd$, donc $g^{|G|} = (g^k)^d = 1^d = 1$. □

Corollaire 11 (Petit théorème de Fermat)**.** *Soit p un nombre premier, et $x \in \mathbb{Z}$. Alors $x^p \equiv x$ mod p. Si p ne divise pas x, alors $x^{p-1} \equiv 1$ mod p.*

Démonstration. On prend $G = (\mathbb{Z}/p\mathbb{Z})^*$, qui est d'ordre $p-1$. Si x n'est pas divisible par p, alors $\overline{x} \in G$, et donc $\overline{x}^{p-1} = \overline{1}$ par le corollaire précédent, ce qui s'écrit $x^{p-1} \equiv 1$ mod p. On obtient $x^p \equiv x$ mod p en multipliant par x.

Si par contre p divise x, alors $x \equiv 0$ mod p, donc certainement $x^p \equiv 0 \equiv x$ mod p. □

Toujours en guise d'application du théorème de Lagrange, voyons maintenant les sous-groupes d'un groupe cyclique fini d'ordre n : par Lagrange, l'ordre d'un tel sous-groupe doit diviser n, et nous allons voir que réciproquement, pour tout diviseur de n, il y a un sous-groupe de cet ordre, et même un seul. Nous avons déjà vu une partie de l'énoncé dans un autre exercice sur les modules, mais ici on va être plus précis (et c'est à retenir).

Théorème 12. *Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n (en notation multiplicative). Soit d un diviseur de n, et écrivons $n = de$. Alors G possède un unique sous-groupe H_d d'ordre d, et de plus*

$$H_d = \langle g^e \rangle = \{x \in G \mid x^d = 1\}.$$

Démonstration. Commençons par montrer que

$$\langle g^e \rangle = \{x \in G \mid x^d = 1\}.$$

En effet, un $x \in G$ peut s'écrire $x = g^k$, par définition. Alors $x^d = g^{kd}$, de sorte que $x^d = 1$ équivaut à $g^{kd} = 1$, c'est-à-dire à $n|kd$. Mais $de|dk$ si et seulement si $e|k$; et si $k = e\ell$, alors $g^k = (g^e)^\ell$, et $x \in \langle g^e \rangle$. Finalement, on constate que $x^d = 1$ équivaut à $x \in \langle g^e \rangle$, d'où l'égalité. On note H_d pour le groupe en question.

Le groupe H_d est cyclique, engendré par g^e, donc son ordre est le plus petit entier k tel que $(g^e)^k = 1$ (lemme du chapitre 1). Mais $g^{ek} = 1$ si et seulement si $n|ek$, donc $d|k$. L'entier k est un multiple de d, donc $k \geq d$; mais $(g^e)^d = g^n = 1$ par Lagrange, donc par minimalité on a $k = d$. On a montré que H_d est d'ordre d.

Montrons enfin l'unicité. Soit H un sous-groupe de G d'ordre d. Alors pour tout $x \in H$, on a $x^d = 1$ par Lagrange ; ceci montre $H \subset H_d$, et par égalité des ordres, $H = H_d$. □

§2 Actions

Définition 13. Soit X un ensemble. Alors $S(X)$ est le groupe de toutes les bijections $X \longrightarrow X$, avec la composition $\circ$ pour loi de groupe, et l'identité pour élément neutre. On l'appelle le *groupe symétrique de X*. Lorsque $X = \{1, 2, \ldots, n\}$, on écrit S_n pour $S(X)$.

Définition 14. On dit que le groupe G *agit* sur l'ensemble X lorsqu'il existe un homomorphisme $\varphi\colon G \longrightarrow S(X)$. On dira parfois que φ est une *action* de G sur X.

En général, on va écrire $g \cdot x$ au lieu de $\varphi(g)(x)$, pour $g \in G$, $x \in X$ (et φ est alors sous-entendu, mais c'est toujours comme ça). Avec cette notation, on a

$$g \cdot (h \cdot x) = (gh) \cdot x\,, \qquad 1 \cdot x = x\,.$$

Il est facile de montrer que, si on a une application $G \times X \longrightarrow X$ notée $(g, x) \mapsto g \cdot x$, et si les deux propriétés ci-dessus sont vérifiées, alors $g \cdot x = \varphi(g)(x)$ où φ est une action unique. Bref, on aurait pu donner une autre définition, et dans certains livres, c'est ce que vous trouverez.

Exemple 15. Le groupe diédral D_8 agit sur $\mathbb{R}^2$. Le groupe S_n agit sur $\{1, 2, \cdots, n\}$.

Exemple 16. On peut prendre $X = G$, avec l'action $g \cdot x = gx$ (multiplication dans G). On dira « l'action de G sur lui-même par multiplication à gauche ». Notons également que, si H est un sous-groupe de H, alors H agit sur G par multiplication, par restriction de l'action précédente.

Exemple 17. Prenons encore $X = G$, avec cette fois-ci $g \cdot x = gxg^{-1}$. Vérifions qu'il s'agit bien d'une action : on a

$$g \cdot (h \cdot x) = g \cdot (hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = (gh) \cdot x\,.$$

D'autres part $1 \cdot x = x$ est évident. C'est bien une action, et nous parlerons de « l'action de G sur lui-même par conjugaison ».

Exemple 18. Prenons $X = \mathscr{P}(G)$, l'ensemble des parties $S \subset G$. Alors on définit une action de G sur X en posant

$$g \cdot S = \{gs \mid s \in S\}\,.$$

Si H est un sous-groupe de G, alors $G/H \subset \mathscr{P}(G)$, et l'action de G sur $\mathscr{P}(G)$ envoie G/H dans lui-même ; en effet si $xH \in G/H$ alors

$$g \cdot (xH) = gxH \in G/H\,,$$

comme on le vérifie (il y a un tout petit calcul à faire ici). Il y a donc une action de G sur G/H, que appellerons *canonique*, et qui est très importante. Si on utilise la notation « avec les barres », alors on a

$$g \cdot \overline{x} = \overline{gx}\,.$$

Définition 19. Supposons que G agit sur X, et soit $x \in X$. Alors *l'orbite de* x, notée $\mathrm{orb}(x)$, est

$$\mathrm{orb}(x) = \{g \cdot x \mid g \in G\}\,.$$

Exemple 20. Dans l'action de G sur lui-même par conjugaison, les orbites s'appellent les *classes de conjugaison*. Elles jouent un grand rôle dans les deux chapitres suivants.

Lemme 21. *Si* $\mathrm{orb}(x) \cap \mathrm{orb}(y) \neq \emptyset$, *alors* $\mathrm{orb}(x) = \mathrm{orb}(y)$. *En conséquence,* X *est l'union disjointe des différentes orbites de* G.

Démonstration. Laissé en exercice, très similaire au lemme ci-dessus sur les classes à gauche. □

Remarque. En fait, la condition $x \in \mathrm{orb}(y)$ est symétrique en x et y, puisque $x = g \cdot y$ équivaut à $y = g^{-1} \cdot x$. On voit facilement qu'elle est aussi transitive, et bien sûr réflexive, en d'autres termes c'est une relation d'équivalence. Les orbites sont les classes d'équivalence, et voilà qui explique pourquoi elles sont disjointes.

Dans le cas où X est fini, on peut donc trouver des éléments $x_1, \ldots, x_k$ tels que

$$X = \mathrm{orb}(x_1) \cup \mathrm{orb}(x_2) \cup \cdots \cup \mathrm{orb}(x_k)\,,$$

une union disjointe. Les x_i ne sont pas uniques du tout : si on prend un $x \in \mathrm{orb}(x_i)$ quelconque, alors $\mathrm{orb}(x) = \mathrm{orb}(x_i)$ (puisque ces deux orbites contiennent toutes les deux l'élément x !).

Il est bien clair que l'action de G préserve les orbites, c'est-à-dire que si $x \in \mathrm{orb}(x_i)$, alors $g \cdot x \in \mathrm{orb}(x_i)$ pour tout $g \in G$. Donc une action de groupe peut souvent s'étudier « orbite par orbite ». On a d'ailleurs le vocabulaire suivant :

Définition 22. L'action de G sur X est dite *transitive* lorsqu'il n'y a qu'une seule orbite. Il est équivalent (mini-exo) de demander que pour tous $x, y \in X$, il existe un $g \in G$ tel que $g \cdot x = y$.

Ce qui précède montre que l'étude des actions de groupe peut en grande partie se ramener à l'étude des actions transitives.

Bref, nous avons saisi l'importance des orbites et de l'action induite sur elles. Or la structure des orbites est très bien comprise. Voyons ça.

Définition 23. Supposons que G agit sur X, et soit $x \in X$. Alors le *stabilisateur* de x pour cette action est

$$\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}\,.$$

C'est un sous-groupe de G.

Exemple 24. Reprenons l'exemple de l'action de G par conjugaison sur lui-même. Le stabilisateur de $x \in G$ est constitué des $g \in G$ tels que $gxg^{-1} = x$, ce qui revient à $gx = xg$. C'est donc le sous-groupe des éléments qui commutent avec x, et on l'appelle en général le *centralisateur de* x *dans* G.

Proposition 25. *On suppose que* G *agit sur* X. *Soit* $x \in X$, *et soit* $H = \mathrm{Stab}_G(x)$. *Alors l'application*

$$\begin{aligned} \theta\colon G/H &\longrightarrow \mathrm{orb}(x) \\ \overline{g} = gH &\mapsto g \cdot x \end{aligned}$$

est bien définie, c'est une bijection, et de plus pour $\sigma \in G$ *et* $\overline{g} \in G/H$ *on a*

$$\theta(\sigma \cdot \overline{g}) = \sigma \cdot \theta(\overline{g})\,.$$

Ici le $\cdot$ fait référence, à gauche, à l'action de G sur G/H, et à droite, à l'action de G sur X. En d'autres termes, on a une identification de $\mathrm{orb}(x)$ avec G/H, qui est compatible avec les actions.

Démonstration de la proposition. Si $\overline{g_1} = \overline{g_2}$, c'est-à-dire $g_1 H = g_2 H$, alors il existe $h \in H$ tel que $g_2 = g_1 h$. Donc

$$g_2 \cdot x = g_1 \cdot (h \cdot x) = g_1 \cdot x$$

puisque $h \in H = \mathrm{Stab}_G(x)$. Ainsi $g_1 \cdot x$ ne dépend que de $\overline{g_1}$, il est donc légitime de le noter $\theta(\overline{g_1})$, et l'application θ est bien définie.

Montrons que θ est surjective, donc prenons $y \in \mathrm{orb}(x)$. Alors $y = g \cdot x$ pour un $g \in G$ par définition, d'où $y = \theta(\overline{g})$.

Montrons que θ est injective, et supposons donc $\theta(\overline{g}_1) = \theta(\overline{g}_1)$, ce qui se traduit par

$$g_1 \cdot x = g_2 \cdot x \,,$$

d'où

$$g_2^{-1} g_1 \cdot x = x \,,$$

ce qui revient à $g_2^{-1} g_2 \in \mathrm{Stab}_G(x) = H$. On en déduit $g_1 H = g_2 H$, ou encore $\overline{g_1} = \overline{g_2}$. Ainsi, θ est une bijection.

Enfin, prenons $\sigma, g \in G$ et calculons

$$\theta(\sigma \cdot \overline{g}) = \theta(\overline{\sigma g}) = (\sigma g) \cdot x = \sigma \cdot (g \cdot x) = \sigma \cdot \theta(\overline{g}) \,.$$

□

Cette proposition est riche de conséquences. Commençons par des résultats de « comptage » :

Corollaire 26. *On a*

$$|\,\mathrm{orb}(x)| = \frac{|G|}{|\,\mathrm{Stab}_G(x)|} \,.$$

En particulier, la taille d'une orbite est un diviseur de l'ordre de G.

Démonstration. C'est la proposition ci-dessus et le théorème de Lagrange. □

Et en conséquence :

Corollaire 27. *On suppose que le groupe fini G agit sur l'ensemble fini X, et on prend x_1, x_2, …, x_k tels que X soit l'union disjointe*

$$X = \mathrm{orb}(x_1) \cup \cdots \cup \mathrm{orb}(x_k) \,.$$

Alors

$$|X| = \sum_i \frac{|G|}{|\,\mathrm{Stab}_G(x_i)} \,.$$

On appelle parfois cette identité « l'équation aux classes ». Il paraît beaucoup moins important de la mémoriser que de mémoriser la proposition.

Démonstration. Bien sûr $|X|$ est la somme des nombres $|\operatorname{orb}(x_i)|$. Or, le corollaire précédent affirme que $|\operatorname{orb}(x_i)| = |G|/|\operatorname{Stab}_G(x_i)$. □

§3 Les théorèmes de Sylow

Définition 28. Soit G un groupe d'ordre n, et soit p un nombre premier. Écrivons $n = p^k m$ avec m premier à p. Alors un *p-Sylow* de G est un sous-groupe H d'ordre p^k.

(Si vous avez beaucoup de temps devant vous, vous pouvez dire « un sous-groupe de Sylow associé au nombre premier p » au lieu de dire « un p-Sylow ».)

Il n'est pas évident du tout, étant donné un groupe G arbitraire, qu'il possède un p-Sylow. Mais c'est ce qu'affirment, entre autres choses, les théorèmes de Sylow que nous allons démontrer.

Nous aurons besoin d'une notation : si H est un sous-groupe de G, et si $g \in G$, sans surprise on pose

$$Hg = \{hg \mid h \in H\}.$$

Le point crucial va être de considérer l'ensemble

$$X = \{A \subset G \text{ tel que } |A| = p^k\}.$$

Ici A n'est pas un sous-groupe, mais juste une partie du groupe G d'ordre $n = p^k m$, comme ci-dessus. On fait agir G sur X par

$$g \cdot A = \{ga \mid a \in A\};$$

en d'autres termes, c'est l'action que l'on a déjà vue de G sur l'ensemble $\mathscr{P}(G)$ de ses parties, sauf qu'on se restreint aux parties de cardinal p^k.

On a alors le lemme suivant, qui détient la clef des théorèmes de Sylow.

Lemme 29. *Dans les notations ci-dessus, soit $A \in X$ et H son stabilisateur. Les conditions ci-dessous sont équivalentes.*

1. $|\operatorname{orb}(A)|$ *est premier à* p.
2. *il existe* $g \in G$ *tel que* $A = Hg$.
3. $\operatorname{orb}(A)$ *contient un unique* p*-Sylow, qui est un conjugué de* H.
4. H *est un* p*-Sylow de* G.
5. $|\operatorname{orb}(A)| = m$.

Démonstration. Supposons (1), et montrons (2). Pour cela, prenons $g \in A$ un élément quelconque. Pour $h \in H$, on a $hg \in hA = A$ puisque H est le stabilisateur de A. Donc $Hg \subset A$. Mais $|Hg| = |H|$, donc on en déduit que $|H| \leq |A| = p^k$. Mais en même temps, $|\operatorname{orb}(A)| = |G|/|H|$ est premier à p, ce qui veut dire que $|H| = p^k r$ avec $r|m$. Au total, on doit donc avoir $r = 1$ et $|H| = p^k$. Puisque $|Hg| = |H| = p^k$, on en déduit $Hg = A$.

Passons à (2) $\implies$ (3). Si $A = Hg$, posons $K = g^{-1}Hg = g^{-1}A$, de sorte que $|K| = |H| = |A| = p^k$, et H et K sont tous les deux des p-Sylow. Mais de plus, $K \in \operatorname{orb}(A)$ par construction, et en fait c'est le seul ensemble dans $\operatorname{orb}(A) = \operatorname{orb}(K)$ qui est un sous-groupe de G (si xK est un sous-groupe, il contient $1 \in G$ d'où $x \in K$ et $xK = K$). C'est donc, en particulier, le seul p-Sylow dans $\operatorname{orb}(A)$. Nous avons (3).

L'implication (3) $\implies$ (4) est triviale. Si on a (4), on écrit $|\operatorname{orb}(A)| = |G|/|H| = m$, donc on a (5). Et (5) $\implies$ (1) est encore trivial. □

Corollaire 30. *Il existe une bijection entre les p-Sylow de G et les orbites de cardinal premier à p dans X, donnée par $H \mapsto \operatorname{orb}(H)$.*

Démonstration. En effet, soit H un p-Sylow, et prenons $A = H$ dans la notation du lemme ; alors $\operatorname{Stab}_G(H) = H$, puisque la condition $gH = H$ équivaut à $g \in H$. Donc $\operatorname{orb}(H)$ est de cardinal premier à p, par l'implication (4) $\implies$ (1). Donc l'application $H \mapsto \operatorname{orb}(H)$ envoie bien le p-Sylow sur une orbite de cardinal premier à p.

Si $\operatorname{orb}(H) = \operatorname{orb}(K)$ où H et K sont tous les deux des p-Sylow, alors par la propriété (3) (la partie unicité, en fait), on a $H = K$; l'application $H \mapsto \operatorname{orb}(H)$ est donc injective.

Enfin, l'implication (1) $\implies$ (3) montre que toute orbite $\operatorname{orb}(A)$ de cardinal premier à p contient un p-Sylow K, mais alors $\operatorname{orb}(K) = \operatorname{orb}(A)$. Ainsi, l'application est également surjective, ce qui termine la démonstration. □

Il va donc être essentiel, pour montrer que G contient au moins un p-Sylow, de comprendre la taille des orbites dans X. Or, on a

$$|X| = \binom{p^k m}{p^k}$$

par définition. Et nous notons :

Lemme 31. *Si $pgcd(m, p) = 1$, où p est premier, alors pour tout $k \geq 0$ on a*

$$\binom{p^k m}{p^k} \equiv m \bmod p\,.$$

Démonstration. On peut le faire en raisonnant avec les nombres binomiaux, c'est un bon exercice. Mais on peut aussi le déduire du lemme précédent (ce n'est pas la fonction principale de ce lemme, mais ça marche).

En effet, prenons $G = \mathbb{Z}/n\mathbb{Z}$, avec $n = p^k m$. Alors G possède un unique p-Sylow, d'après le théorème 12. Donc le lemme ci-dessus avec son corollaire nous dit qu'il existe une unique orbite de G dans X dont le cardinal est premier à p, et que ce cardinal est m. Si les orbites

sont $\mathrm{orb}(A_1), \ldots, \mathrm{orb}(A_k)$, avec $|\mathrm{orb}(A_1)| = m$ et $\mathrm{orb}(A_i)$ divisible par p pour $i \geq 2$, on a bien

$$|X| \equiv |\mathrm{orb}(A_1)| \text{ mod } p\,.$$

□

Il est maintenant très facile d'établir :

Théorème 32 (Premier théorème de Sylow)**.** *Soit G un groupe fini et p un nombre premier. Alors G possède un p-Sylow.*

Démonstration. En vue du corollaire au premier lemme, il faut montrer qu'il existe une orbite de cardinal premier à p, dans l'action de G sur X. Supposons par l'absurde que, les orbites étant $\mathrm{orb}(A_1), \ldots, \mathrm{orb}(A_k)$, chaque nombre $|\mathrm{orb}(A_i)|$ soit divisible par p. Alors $|X| = \sum_i |\mathrm{orb}(A_i)|$ est également divisible par p. Or c'est impossible, puisque $|X|$ est congru à m modulo p, où $pgcd(m, p) = 1$. □

Théorème 33 (Deuxième théorème de Sylow)**.** *Soit H un p-Sylow de G, soit K un sous-groupe de G qui est un p-groupe, et soit H un p-Sylow de G. Alors il existe $g \in G$ tel que $gKg^{-1} \subset H$. Si K est lui-même un p-Sylow, on en déduit que $gKg^{-1} = H$, et donc que tous les p-Sylow sont conjugués entre eux.*

Rappelons qu'un groupe fini est appelé un *p-groupe* lorsque son ordre est une puissance de p.

Démonstration. Sous forme d'exercices. □

Théorème 34 (Troisième théorème de Sylow)**.** *Soit n_p le nombre de p-Sylow distincts du groupe G d'ordre $p^k m$, avec $pgcd(m, p) = 1$. Alors*

- *n_p divise m,*
- *$n_p \equiv 1$ mod p.*

Démonstration. Le premier point va être une conséquence du deuxième théorème de Sylow. En effet, soit S l'ensemble des p-Sylow de G, de sorte que S est de cardinal n_p par définition. Le groupe G agit sur S par conjugaison (il est clair que si H est un p-Sylow, alors gHg^{-1} aussi), et le théorème précédent nous dit que cette action est transitive (= ne possède qu'une seule orbite). Si H est un p-Sylow, notons N son stabilisateur dans cette action. On a alors

$$n_p = |S| = |\mathrm{orb}(H)| = |G|/|N|\,.$$

Une remarque simple est alors que $H \subset N$ (en d'autres termes, si $h \in H$ alors $hHh^{-1} = H$, ce qui est évident). Finalement on a $H \subset N \subset G$, avec H d'ordre p^k et G d'ordre $p^k m$. Par Lagrange, l'ordre de N est $p^k r$ avec $r|m$. On conclut effectivement que

$$n_p = \frac{m}{r}\,,$$

ou encore $m = r n_p$.

Passons au deuxième point. Par le corollaire au premier lemme, il y a n_p orbites de cardinal premier à p dans l'action de G sur X, et ces orbites sont toutes de cardinal m par le lemme lui-même. L'union (disjointe) de ces orbites contient donc mn_p éléments de X, alors que les autres orbites sont de cardinal divisible par p. On a donc $|X| \equiv mn_p \mod p$. Mais on sait également que $|X| \equiv m \mod p$, d'où

$$m \equiv mn_p \mod p\,.$$

Puisque m est premier à p, l'élément $\overline{m}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$, donc on peut simplifier par m pour obtenir $\overline{n_p} = \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. □